IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

USA,

Plaintiff,

v.

WESLEY STEVEN BOHANNON,

Defendant.

Case No. 19-cr-00039-CRB-1

ORDER DENYING MOTION TO SUPPRESS

Defendant Wesley Bohannon has been charged with possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B), (b)(2). He now moves to suppress the fruits of: (1) Microsoft's automated search of files that Bohannon uploaded to his cloud storage account, which resulted in Microsoft reporting the presence of a child pornography image to the National Center for Missing & Exploited Children (NCMEC); (2) NCMEC's visual inspection of the image and identification of an office at California State University as the owner of the IP address associated with the Microsoft account; (3) San Francisco Police Department (SFPD) Sergeant Christopher Servat's visual inspection of the image; and (4) the SPFD's execution of a search warrant that authorized the SFPD to search Bohannon's Microsoft account.

The Court heard argument from the parties on December 9, 2020. The Court hereby denies Bohannon's motion to suppress.

I. BACKGROUND

Microsoft is a private company that, among many other businesses, offers consumers a cloud file storage service called OneDrive. OneDrive allows users to upload digital files and access those files across devices. See Mot. to Suppress (dkt. 63) at 2.

Microsoft's "Code of Conduct" requires OneDrive users to agree not to engage in unlawful acts or "any activity that exploits, harms, or threatens to harm children." See Services Agreement (dkt. 71-3) at 135. It also states that Microsoft "reserves the right to review Your Content" when "investigating alleged violations of these terms." Id. Microsoft's Services Agreement requires users to agree to "consent to Microsoft's collection, use, and disclosure" of their content and data "as described in [a] Privacy Statement." Id. at 160. The Privacy Statement informs users that Microsoft will "access, transfer, disclose, and preserve personal data, including . . . files in private folders on OneDrive" when Microsoft has "a good faith belief that doing so is necessary to . . . enforcing the terms governing the use of the services." Privacy Statement (dkt. 71-4) at 422–23.

The National Center for Missing & Exploited Children (NCMEC), a nonprofit corporation, operates a "CyberTipline" that receives reports of child sexual exploitation, including child pornography. See Shehan Affidavit (dkt. 71-1) ¶¶ 2–3. Microsoft has supported NCMEC in various ways. For example, Microsoft helped found NCMEC's "public-private Technology Coalition," which is meant to "facilitate information-sharing and cooperation among industry and law enforcement." Mot. to Suppress at 7 (citation omitted). And although NCMEC is "primarily financed by the U.S. Department of Justice . . . Microsoft has made donations to NCMEC worth millions of dollars over the years." Id. at 8.

Whenever Microsoft obtains "actual knowledge" that a user's conduct constitutes an "apparent violation" of certain statutory provisions criminalizing offenses relating to child pornography, federal law requires Microsoft to report information about the violation to NCMEC's CyberTipline. See 18 U.S.C. § 2258A(a)–(b). NCMEC has broader obligations than Microsoft—federal law requires "its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways." United States v. Ackerman, 831 F.3d 1292, 1296 (10th Cir. 2016). For example, NCMEC has statutory obligations to maintain the CyberTipline or its equivalent and to forward any report it receives to law enforcement agencies. 18 U.S.C. § 2258A(c).

On December 14, 2017, Microsoft submitted a "CyberTip" to NCMEC stating that Microsoft had located child pornography on a user's OneDrive account eight days earlier. See CyberTip Report (dkt. 64-1) at WSB-192. Microsoft's PhotoDNA system, which uses image file hash values to automatically compare users' uploaded images to known child pornography images, had identified the child pornography. See id. at WSB-193; Mot. to Suppress at 2 (citing Microsoft PhotoDNA, at https://www.microsoft.com/en-us/photodna (October 9, 2020)). According to Microsoft's Head of Digital Safety Operations Sean Davis, Microsoft uses PhotoDNA to "keep individuals and families safer and more secure online" as part of its broader effort to "deliver secure, private, and reliable computing experiences." Davis Decl. (dkt. 71-2) ¶¶ 2–3. PhotoDNA contributes to a "safer online environment" by helping Microsoft "find and remove images of child sexual abuse from Microsoft's online services." Id. ¶ 4. Although Microsoft developed PhotoDNA to serve its "business interests," Microsoft complies with its statutory obligation to report any child pornography it identifies to NCMEC. Id. ¶¶ 5, 11. Here, before submitting the CyberTip, Microsoft had not communicated with NCMEC or any government agency regarding its use of PhotoDNA in relation to this OneDrive account. See id. ¶¶ 4–5, 12–13. But Microsoft has separately "donated" the PhotoDNA system to NCMEC and to law enforcement entities. See Mot. to Suppress at 2–3; Davis Decl. ¶ 14. And in general, Microsoft and NCMEC have continued to work together to improve the PhotoDNA system's database and technology. See Mot. to Suppress at 8–9.

Microsoft's CyberTip categorized the image as depicting a "prepubescent minor" engaging in "sexually explicit conduct." CyberTip Report at WSB-192, 194. The CyberTip also disclosed a numeric username and IP address associated with the OneDrive account. Id. at WSB-190. NCMEC identified the owner of the IP address as an office at California State University, and an NCMEC analyst "viewed the uploaded files" and confirmed that the image was child pornography. See CyberTip Report at WSB-194, 196. Consistent with its own statutory obligations, see 18 U.S.C. § 2258A(c), NCMEC forwarded the CyberTip and information regarding the owner of the IP address to local law

enforcement in a CyberTip Report. Id. at WSB-198.

San Francisco Police Department Sergeant Christopher Servat was assigned the CyberTip Report on January 2, 2018—27 days after Microsoft identified the child pornography and 19 days after Microsoft submitted the CyberTip—and applied for a search warrant on January 4, 2018. See Warrant Application (dkt. 64-2) at WSB-58–59. Servat's warrant application stated that he had received the CyberTip, that the listed IP address had been "geo-located" to San Francisco, that Servat had reviewed the uploaded file and confirmed that it was child pornography, and that based on his "training and experience" (which he described), the child pornography would be located in the "above premises," referring to the OneDrive account. Id. at WSB-58–59.[1] The warrant application clarified that the purpose of the investigation was to "identify and arrest" the person who had stored the child pornography on the OneDrive account. Id. at WSB-59. The application did not disclose the precise date that Microsoft had identified the child pornography. Id. at WSB-58–59; CyberTip Report at WSB-192.

Based on Servat's warrant application, a Superior Court of California magistrate judge issued Servat's requested search warrant. See Warrant (dkt. 64-2) at WSB-57. The warrant granted permission to search Microsoft's digital records for "all account information," including "subscriber names, user names, and other identities." Id. at WSB-56. It also granted permission to search "all content" in the OneDrive account. Id. Finally, the warrant granted permission to search all "images, links [and] videos uploaded and saved on [the] account from 7/1/2017 to 1/3/2018," which was redundant given its permission to search all content in the account. Id. at WSB-56–57.

Servat received the contents of the OneDrive account for review on March 7, 2018. SFPD Investigation Rpt. (dkt. 64-3) at WSB-45–52. Examining the files, Servat found over five hundred child pornography images. Id. at WSB-46. Servat also found numerous

[1] The warrant application also requested that the search warrant command "the search of the person, premise(s) or vehicle(s) designated above," also referring to the OneDrive account. Warrant Application at WSB-59.

documents authored by a person named "Wesley" and a letter purporting to be authored by "Wesley Bohannon." Id. at WSB-46. In the same folder as the child pornography images, Servat found several "selfie" photographs of an adult male with gray hair and a grey beard. Id. at WSB-47. These pictures matched Wesley Bohannon's mugshot and driver's license. Id. at WSB-48.[2]

On March 15, 2018, SFPD officers arrested Bohannon and seized a cell phone and laptop that he was carrying; law enforcement eventually searched the devices, discovering more child pornography. Id. at WSB-48–49. On January 22, 2019, Bohannon was indicted for one count of possession of child pornography based on these materials. See Indictment (dkt. 1).

II. LEGAL STANDARD

Under the Fourth Amendment, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV. Unless an exception applies, the exclusionary rule prevents unlawfully obtained evidence from being introduced at trial against the person whose Fourth Amendment rights were violated. See Mapp v. Ohio, 367 U.S. 643, 655 (1961). This includes other evidence "come at by exploitation of that illegality." Wong Sun v. United States, 371 U.S. 471, 488 (1963) (quotation omitted).

III. DISCUSSION

Bohannan moves the Court to suppress the fruits of any searches conducted by Microsoft and NCMEC, which includes all evidence of child pornography images obtained in later searches. See Mot. to Suppress at 1, 10–12, 14. Bohannon also moves to suppress the fruits of Servat's visual inspection of the image, and the SFPD's execution of the search warrant. Id. at 13–23.

The Court denies Bohannon's motion. First, the Fourth Amendment does not apply to Microsoft's search, as Microsoft was not acting as a government entity or agent. Even if

[2] Servat used this and other information to obtain additional search warrants not at issue here. See Mot. to Suppress at 4 & n.5.

the Fourth Amendment applied, Bohannon consented to Microsoft's search by agreeing to Microsoft's terms of service. Second, NCMEC did not conduct any search and thus could not have violated Bohannon's Fourth Amendment rights. Third, when Sergeant Servat confirmed that the image was child pornography, this did not result in any further intrusion on Bohannon's privacy. Finally, the SFPD's warrant was supported by probable cause, and were it not, the good faith exception to the exclusionary rule would apply because law enforcement reasonably relied on the warrant.

A. Microsoft's PhotoDNA Search

Bohannon argues that Microsoft's initial identification of child pornography in the OneDrive account resulted from an unlawful warrantless search. But the Fourth Amendment does not apply to Microsoft's private actions and, in any event, Bohannon consented to Microsoft searching his account.

The Fourth Amendment's protection against unreasonable searches does not apply to a search "by a private individual not acting as an agent of the government or with the participation or knowledge of any government official." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citation omitted). By contrast, "[w]here a private party acts as an 'instrument or agent' of the state in effecting a search or seizure, Fourth Amendment interests are implicated." Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

A defendant "has the burden of establishing government involvement in a private search." United States v. Cleaveland, 38 F.3d 1092, 1093 (9th Cir. 1994). The "relevant inquiry is: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends." Id. (quoting United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994)). At the second step, a private entity may have "dual motives" comprising both a "legitimate, independent motivation to further its own ends" and a desire to assist law enforcement. Id. at 1094 (citation omitted). If that is the case, the Ninth Circuit requires the Court to determine whether "the government's participation" in the search was "so extensive as to trigger Fourth Amendment scrutiny." Id. It is not enough that the

government "used the fruits of [the] search to obtain a warrant." Id. Instead, the government must have "actively" participated in the search. Id.; see also United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981) ("The presence of law enforcement officers who do not take an active role in encouraging or assisting an otherwise private search has been held insufficient to implicate Fourth Amendment interests, especially where the private party has had a legitimate independent motivation for conducting the search."); Corngold v. United States, 367 F.2d 1, 5–6 (9th Cir. 1966) (en banc) (explaining that even when a private party has dual motives, a search that law enforcement "joined actively" is equivalent to a search by the government).

Microsoft is a private party and was not acting as a government agent or instrument when it used PhotoDNA to identify child pornography in Bohannon's OneDrive account. First, Bohannon does not allege that the government knew about this PhotoDNA search, and Microsoft's general practice of using PhotoDNA to identify child pornography—a practice that it has no statutory obligation to perform—is not enough. See United States v. Green, 857 F. Supp. 2d 1015, 1018 (S.D. Cal. 2012). If it were, anything that private persons routinely do and that helps prevent crime could constitute government action. Second, Bohannon has not shown that Microsoft's "legitimate, independent motivation to further its own ends" was "negated" by Microsoft's potential "dual motive to detect or prevent crime." Cleaveland, 38 F.3d at 1094. Through its Head of Digital Safety Operations, Microsoft has articulated various significant and undisputed business justifications for its efforts to combat child pornography online. Davis Decl. ¶¶ 2–4. These justifications relate to user experiences and Microsoft's brand, and thus go well beyond merely "preventing criminal activity." United States v. Reed, 15 F.3d 928, 932 (9th Cir. 1994). Even if Microsoft is also happy to help law enforcement prevent child sexual abuse and has a "track record" of doing so, Mot. to Suppress at 11, there was no "government involvement" in this PhotoDNA search, let alone the active or "extensive" participation necessary to override Microsoft's "legitimate, independent motive." Cleaveland, 38 F.3d at 1094.

Bohannon seeks to avoid this result by conflating Microsoft's conduct with NCMEC's conduct. Bohannon argues that because "Microsoft and NCMEC jointly developed, maintain, and controlled the very technology that was used to conduct the search in this case," and because courts have held that NCMEC sometimes acts as a government agent in related contexts, the PhotoDNA search here constitutes government action. Mot. to Suppress at 11–12 (citing Ackerman, 831 F.3d at 1296–97). This argument fails. NCMEC did not conduct the PhotoDNA search. And even if NCMEC is properly considered a government entity, Ackerman, 831 F.3d at 1296–97, the same can hardly be said for Microsoft.[3] Nor did NCMEC play the principal to Microsoft's agent here. NCMEC's participation in this series of investigations began when Microsoft sent NCMEC a CyberTip. NCMEC is related to the initial PhotoDNA search only to the extent that NCMEC (along with various other entities) (1) has helped Microsoft build and improve the PhotoDNA system, and (2) uses PhotoDNA now for its own purposes. See Mot. to Suppress at 11–12; Davis Decl. ¶ 14. That does not mean that NCMEC required, directed, actively participated in, or even knew about this search. See Cleaveland, 38 F.3d at 1093. At bottom, the inquiry is whether Bohannon has carried his burden of showing that Microsoft acted as an "instrument or agent" of NCMEC or another government entity while searching Bohannon's OneDrive account. Coolidge, 403 U.S. at 487. Microsoft's general, mutually beneficial relationship with NCMEC, even as it relates to the technology at issue, is not enough.[4]

---

[3] Bohannon does not allege that like NCMEC, Microsoft is obligated to maintain an information gathering system and report results to law enforcement. See 18 U.S.C. § 2258A(c). Microsoft must report information to NCMEC when it has actual knowledge of child pornography, see 18 U.S.C. § 2258A, but is not required to maintain a sophisticated system for obtaining such knowledge. Microsoft also lacks NCMEC's statutory power to (for example) "call on various federal agencies for unique forms of assistance in aid of its statutory [law enforcement] functions." Ackerman, 831 F.3d at 1296 (citing 18 U.S.C. § 3056(f)). Thus, Congress has given NCMEC, but not Microsoft, "special law enforcement duties and powers" that "no other private person has." Id. By conferring those duties and powers on NCMEC, and largely funding NCMEC's budget, Congress exercises a "sort of 'day-to-day' statutory control over [NCMEC's] operations," which cannot be said for Microsoft. Id. at 1298.

[4] Courts overwhelmingly agree that when technology companies search user accounts in a similar manner, they do not act as government agents. See United States v. Stevenson, 727 F.3d 826, 831 (8th Cir. 2013); United States v. Cameron, 699 F.3d 621, 636–38 (1st Cir. 2012); United States v.

Bohannon's argument that the PhotoDNA search was unlawful fails for another, independent reason: he consented to the search. Government agents may search a constitutionally protected area when they have a warrant supported by probable cause. See Katz v. United States, 389 U.S. 347, 357–358 (1967). Searches conducted without such a warrant are unreasonable, "subject only to a few specifically established and well-delineated exceptions." Id. at 357. "Consent" is one such exception—with it, the government needs neither a warrant nor probable cause. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). Here, even if Microsoft were acting as a government agent, Bohannon consented to Microsoft's PhotoDNA search by agreeing to Microsoft's terms of service. See Services Agreement at 135, 160; Privacy Statement at 422–23. Bohannon agreed that Microsoft could "access" and "disclose" his "personal data," including his "private folders on OneDrive," so long as Microsoft believed in good faith that doing so was necessary to enforcing its terms of service, Privacy Statement at 422–23, including its prohibition on unlawful acts and "any activity that exploits, harms, or threatens to harm children," Services Agreement at 135. That is precisely what happened here. Thus, even were Microsoft acting as a government agent, its PhotoDNA search was reasonable under the Fourth Amendment.

For both reasons, Microsoft's initial identification of a child pornography image in Bohannon's OneDrive account was lawful.

B. NCMEC's IP Address Investigation

Next, NCMEC matched the IP address associated with the OneDrive account to an IP address owned by an office at California State University. See CyberTip Report at WSB-194, 196. Bohannon argues that NCMEC "assumed a law enforcement role" by "investigating the IP address and forwarding information concerning the location and owner of the IP address to SFPD." Mot. to Suppress at 12. But assuming that NCMEC was acting as a government entity or agent, this conduct involved no Fourth Amendment

---

Richardson, 607 F.3d 357, 366 (4th Cir. 2010); United States v. Wolfenbarger, 16-CR-00519-LHK, 2019 WL 6716357 (N.D. Cal. Dec. 10, 2019).

search.

The "capacity to claim the protection of the Fourth Amendment" depends on "whether the person who claims the protection of the Amendment has a legitimate expectation of privacy" that the government is alleged to have violated. Rakas v. Illinois, 439 U.S. 128, 143 (1978). Bohannon does not allege that NCMEC invaded some legitimate expectation of privacy, belonging to him, by matching the IP address associated with the OneDrive account to an owner. And without such an invasion, it makes no difference whether NCMEC's investigation resembled one that law enforcement might conduct. Thus, NCMEC's conduct linking the IP address to an owner and passing that information to the SFPD was lawful under the Fourth Amendment.

C. NCMEC and Servat's Visual Image Inspections

Bohannon argues that when Servat (and presumably NCMEC before him) visually inspected the image that prompted the CyberTip, these constituted additional warrantless searches that may have been unlawful if nobody at Microsoft had already inspected the image. See Mot. to Suppress at 22. Although the CyberTip indicates that someone at Microsoft viewed the "entire contents of [the] uploaded file," see Cybertip Report at WSB-192, and the government confirms that "someone at Microsoft reviewed the image before it was submitted to NCMEC," Opp. at 3 (citing Shehan Affidavit ¶ 15; Davis Decl. ¶ 15), Bohannon alleges that "the company did not actually review the image in the OneDrive account, it merely examined the associated hash" used to link the image to known child pornography, Reply at 14. Bohannon argues that subsequent visual inspections thus unlawfully "exceeded the scope of Microsoft's initial intrusion." Mot. to Suppress at 22.

The Court need not resolve whether someone at Microsoft opened and looked at the image file in the OneDrive account. Even if Microsoft examined only the "associated hash" before passing the document on to NCMEC, "hash values are specific to the makeup of a particular image's data." United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018). That means examining the hash values to locate a known compared image is equivalent to examining the image itself. NCMEC did not open a "virtual container" like a file folder or

an email that could have contained both the image and "any number of private and protected facts." Ackerman, 831 F.2d at 1306. NCMEC simply viewed the image. Further, because Microsoft had the lawful and practical ability to view and disclose the image, "frustration" of Bohannon's "original expectation of privacy" had already occurred. United States v. Tosti, 733 F.3d 816, 821 (9th Cir. 2013). Thus, assuming that NCMEC was acting as a government agent when a person at NCMEC inspected the image, see Ackerman, 831 F.3d at 1296–97, the inspection constituted "governmental use of . . . now non-private information," not a separate search, Tosti, 733 F.3d at 821. And because someone at NCMEC indisputably inspected the image, Servat's visual inspection could not have caused any further intrusion.[5]

D. The Search Warrant

Bohannan argues that Servat's warrant application did not establish probable cause to search the items listed in the warrant, id. at 14–19, and (in the alternative) that the application recklessly or intentionally omitted information material to the magistrate's probable cause finding, id. at 19–23. But the warrant was supported by probable cause, such that any omission was immaterial.

Servat's warrant application summarized the CyberTip, explained that the IP address was located in San Francisco, confirmed that Servat had reviewed the image and determined that it was child pornography, and suggested based on Servat's training and experience that the child pornography would be located on the same OneDrive account where it was originally identified. See Warrant Application at WSB-58–59. The application also explained that the investigation's purpose was to "identify and arrest" the

[5] Relatedly, under the so-called "third-party doctrine," the Supreme Court has held that individuals lack any reasonable expectation of privacy in materials they choose to share with third parties. See, e.g., United States v. Miller, 425 U.S. 435, 440–43 (1976); Smith v. Maryland, 442 U.S. 735, 742–46 (1979). The Court need not extend this doctrine to the full contents of a cloud storage account to conclude that it applies here. Bohannon agreed that Microsoft could search his OneDrive account for, gain access to, and disclose this particular type of content—child pornography that violates Microsoft's terms of service. Thus, to the extent that Bohannon had a subjective expectation of privacy in the child pornography image, that expectation was not objectively reasonable.

person who possessed the child pornography. Id. at WSB-59. Bohannon argues that the search warrant was not supported by probable cause because Servat's warrant application did not (1) describe when or how Microsoft had identified the child pornography image or associated it with the OneDrive account, (2) expressly state that child pornography might be stored indefinitely on a monthly paid file-hosting service like OneDrive, (3) inform the Court that NCMEC had identified the apparent owner of the IP address, or (4) propose a protocol for sifting through the requested data. See Mot. to Suppress at 3–4.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." Ornelas v. United States, 517 U.S. 690, 696 (1996). This "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." District of Columbia v. Wesby, 138 S. Ct. 577, 586 (2018) (quoting Illinois v. Gates, 462 U.S. 213, 243–44 n.13 (1983)). Whether a magistrate "had a substantial basis for concluding that probable cause existed" is reviewed for "clear error" and with "great deference." United States v. Schesso, 730 F.3d 1040, 1045 (9th Cir. 2013).

Here, the magistrate did not clearly err in finding a fair probability that evidence of possession of child pornography, or who had possessed that child pornography, would be located on the OneDrive account and in the account information. That the warrant application did not state when Microsoft had identified the image presents the closest question arising from Bohannon's motion. See Mot. to Suppress at 16–17. The warrant application did not indicate that people who use services like OneDrive store child pornography indefinitely, likely because the child pornography had been discovered less than one month before Servat submitted the warrant application. But were law enforcement seeking only the child pornography image in the OneDrive account, the Court would still need to determine whether the warrant application's failure to expressly state the date on which Microsoft identified the image is fatal to the magistrate's probable cause finding.

That is not the case here. Law enforcement sought not only evidence of child

pornography, but also evidence that would help them "identify and arrest" a then-unknown OneDrive user who had possessed child pornography. See Warrant Application at WSB-59. For that reason, the magistrate granted permission to search both the content in the account, which might contain clues as to the unknown person's identity, and account information like "subscriber names, user names, and other identities." Warrant at WSB-56. The evidentiary value of the account holder's identity—and thus who had likely used the OneDrive account to store child pornography—distinguishes this case from others in which law enforcement knew who owned a computer and merely sought to find child pornography on that computer. See, e.g., United States v. Lacy, 119 F.3d 742, 745–46 (9th Cir. 1997). Regardless whether people tend to keep child pornography in cloud storage accounts for long periods of time, there is a commonsense probability that such accounts contain evidence probative to discovering who used the account to store child pornography in the past. And a magistrate could draw that obvious inference without the warrant application expressly stating it. See United States v. Elliott, 322 F.3d 710, 716 (9th Cir. 2003) ("A magistrate is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense.") (citation omitted).

Although this conclusion is enough to support the magistrate's probable cause determination, the Court would also conclude that the warrant application supported a finding of probable cause that the child pornography image would be in the OneDrive account. Twenty-three years ago, the Ninth Circuit stated in dictum that it was "unwilling to assume that collectors of child pornography keep their materials indefinitely." Lacy, 119 F.3d at 746. But Lacy nonetheless held that a warrant application stating that collectors of child pornography "rarely if ever dispose of such material, and store it for long periods" established probable cause. Id. (citation omitted). In the time since Lacy, officers applying for warrants have typically included similar "boilerplate" language explaining that people who possess child pornography tend to keep it for long periods. See, e.g., Schesso, 730 F.3d at 1047; United States v. Hay, 231 F.3d 630, 635–36 (9th Cir.

2000).

Lacy's dictum does not control the question whether there is a fair probability that child pornography located in a cloud storage account at one point might still be there. By now, that people who collect child pornography tend to keep their materials for long periods is arguably a matter of common sense that any magistrate could infer. See Schesso, 730 F.3d at 1047 (collecting cases with similar "boilerplate" statements indicating that people tend to keep child pornography for long periods, and holding that delays of eighteen months and three years between known conduct relating to child pornography and the issuance of a search warrant did not defeat probable cause). Further, computing technology has changed dramatically since Lacy in ways that make it easier to store digital files indefinitely, the advent of cloud storage being just one example. Therefore, Lacy does not prevent the Court from holding that the past presence of child pornography in a cloud storage account creates a fair probability, if not a certainty, that child pornography is currently located in the account.

Regardless, a reasonable magistrate could infer from the warrant application that Microsoft had discovered the child pornography in this OneDrive account recently. The application noted that Servat had been assigned the CyberTip on January 2, 2018—just two days earlier. It may be true that "CyberTip reports may languish for months or years before an investigator receives or follows up on them." Mot. to Suppress at 16–17. But a reasonable magistrate could infer that even if material delays can conceivably occur between the discovery of child pornography and the assignment of a CyberTip, no such delay had occurred here.[6] Indeed, the warrant application averred that it contained "all

[6] At the hearing, the parties disputed whether the warrant document incorporated additional facts (not contained in the warrant application) supporting a probable cause finding. The confusion arises from the search warrant document comprising both a warrant and an affidavit—these being separate from an "attached and incorporated" statement of probable cause. See Warrant at WSB-57. In this order, the Court assumes that it can consider only facts in the statement of probable cause (which the Court refers to as the "warrant application") to determine whether the warrant was supported by probable cause. The Court notes that the warrant document twice mentions searching for information under a specific date range—July 1, 2017 to December 3, 2018—of approximately six months leading up to the warrant application. Warrant WSB-56–57. But the Court's analysis in no way relies on this date range.

known material facts," including any "exculpatory" information, further indicating that any material delay would have been disclosed. Warrant Application at WSB-58–59.[7]

Bohannon's other arguments challenging probable cause are meritless. The warrant application's omissions regarding (1) how Microsoft identified the image; and (2) NCMEC's identification of the IP address owner, could not have affected the magistrate's probable cause finding. Given PhotoDNA's undisputed reliability and Servat's confirmation that the image was child pornography, Microsoft's use of PhotoDNA to locate the image had no bearing on the probability that evidence would be found in the OneDrive account. Nor has Bohannon explained how information regarding the IP address owner (an office at California State University, not some other individual) would have detracted from or otherwise affected the likelihood that evidence of child pornography or who possessed it would be found in the OneDrive account.

For the same reasons, the warrant application did not intentionally or recklessly omit anything material to a probable cause finding. See Mot. to Suppress at 19-23 (citing Franks, 438 U.S. at 155–56). Indeed, had Servat included the information that Bohannon describes, the evidence supporting a probable cause finding would have been overwhelming. That evidence would have shown that Microsoft identified the image less than one month before Servat applied for the warrant and that only an office at California State University, and no specific individual, had been linked to the IP address associated with the OneDrive account. See Mot. to Suppress at 15.

Finally, the Court rejects Bohannon's two additional and interrelated arguments regarding probable cause and the scope of the search warrant. First, Bohannon argues that Servat's warrant application did not "propose any protocol for filtering the entire contents" of the OneDrive Account, Mot. to Suppress at 13, and thus did not "identify with particularity the premises to be searched," Reply at 8. Second, Bohannon argues that

[7] Any material delay could have arguably constituted a material omission under Lacy and Franks v. Delaware, 438 U.S. 154 (1978), but Bohannon does not and could not argue that there was a material delay given that Servat applied for the warrant less than a month after Microsoft identified the child pornography.

because the application was so general, there was not probable cause to search the specific items listed in the warrant, including "all content" in the OneDrive account and all "account information." Reply at 9.

The Fourth Amendment requires that "no warrants shall issue" but those based on probable cause "and particularly describing the place to be searched." U.S. Const. amend. IV. Of particular concern to the framers were those "general warrants" that had given "officers of the crown . . . blanket authority to search where they pleased for goods imported in violation of the British tax laws." Stanford v. State of Texas, 379 U.S. 476, 481 (1965). Consistent with this purpose, particularity regarding the places or items to be searched is required "in the warrant." Groh v. Ramirez, 540 U.S. 551, 557 (2004). Separately, the warrant application must establish probable cause to search "all the items of a particular type described in the warrant." In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 857 (9th Cir. 1991).

Here, Servat's warrant application referred to a specific OneDrive account, averred that evidence would be "located at the above premises," and requested permission to search "the person, premise(s) or vehicles designated above for the property or things described." Warrant Application at WSB-59–60. The warrant then granted law enforcement permission to search for:

> -All account information, subscriber names, user names, and other identities
> -Email addresses, telephone numbers, and other contact information associated with [the] account
> -Length of service of [the] account
> -IP connection log history of user access from 7/1/2017 and 1/3/2018, and IP log information relating to account creation
> -All content in OneDrive account
> -All images, links, videos uploaded and saved on account from 7/1/2017 and 1/3/2018.

Warrant at WSB-56.

There is no particularity issue here. Any reasonable reader would understand the warrant application's inartful but clear reference to the specific OneDrive account. More

important, whether the application was overly general is not relevant to the particularity inquiry. Groh, 540 U.S. at 557. As Bohannon acknowledges, the actual warrant was "quite specific about the scope of the search." Reply at 9. To the extent that the warrant described the account information in slightly general terms, a "more precise description [was] not possible" given that neither Servat nor the magistrate could have known precisely where in the OneDrive account evidence would be stored. Lacy, 119 F.3d at 746.

The warrant application also established probable cause to search all the items listed in the warrant. See Reply at 9 (citing In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d at 857). As discussed above, Servat sought evidence of child pornography and the identity of who possessed it. Because the uploaded image provided probable cause to believe that whoever owned the OneDrive account "was a child pornography collector," it gave law enforcement probable cause to search the OneDrive account "for any evidence of possession of or dealing in child pornography." United States v. Schesso, 730 F.3d 1040, 1049 (9th Cir. 2013). And unlike other cases in which the account owner's identity was known, see, e.g., United States v. Hill, 459 F.3d 966, 968–69, 975 (9th Cir. 2006), the evidentiary value of the account owner here justified a broader search including account information. In sum, Bohannon has not explained why the magistrate clearly erred in concluding that there was probable cause to search the full OneDrive account and pertinent account information.

E. Good Faith

Because the warrant was supported by probable cause, there is no need to examine whether the "good faith" exception applies. See United States v. Leon, 468 U.S. 897 (1984). That said, the good faith exception provides an alternative ground for denying Bohannon's motion.

Under Leon, "objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." Id. at 922. This good faith exception cannot apply if (1) the warrant application contained information that the

"affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) "the issuing magistrate wholly abandoned his judicial role," (3) the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or (4) the warrant was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers [could not] reasonably presume it to be valid." Id. at 923 (citation omitted).

For substantially the same reasons that the Court holds that the search warrant was supported by probable cause, law enforcement officers "relied on the search warrant in an objectively reasonable manner." United States v. SDI Future Health, Inc., 568 F.3d 684, 706 (9th Cir. 2009). Bohannon does not contend that the warrant application contained false information. And, given the other content in the warrant application, any deficiency was not so obvious as to render belief in probable cause entirely unreasonable.

IV. CONCLUSION

For the foregoing reasons, the Court denies Bohannon's motion to suppress.

IT IS SO ORDERED.

Dated: December 11, 2020

CHARLES R. BREYER
United States District Judge

United States District Court
Northern District of California